Dear colleagues,

The ETSI Special Task Force on PDF Advanced Electronic Signatures (PAdES - STF 364) is currently looking into the demand for standardization of visible electronic signatures that are part of digital documents. This will play an essential role in our future activities on standardization of electronic signatures inside PDF documents.

By visible signatures we mean the graphical elements such as text and images that would visually represent to a human the act of signing and would be linked to an electronic signature. They may contain information about that electronic signature and be associated with a defined location inside the document.

We would appreciate any input to one or more of the following questions.

1) Do you know of requirements in the context of visible electronic signatures?
2) Are you aware of activities on visible signatures?
3) What are the requirements for standardization on the area of visible signatures?

The STF identified the following issues from initial discussions, on which views are also sought:

A) **Trust in the visible electronic signature**: Since some document formats, such as PDF, allow for arbitrary graphics as part of the page's content, there is no known way of verification of the visible signature (as unique from other page content) when verifying an electronic signature. Ordinary document content including the visible signature can always be made up when signing a document that, although associated with an electronic signature, need not necessarily truly represent that signature. We consider that trust for the verifier into the content of the visible signature can only be created by verifying the electronic signature represented outside the electronic document. As an example, the trustworthy verification result can only be displayed in the user interface of a document viewer outside of the context in which the document is displayed.

B) **Building Visible Signature from Electronic Signature**: The visible electronic signature may or may not contain information about the electronic signature such as the common or distinguished name of the signer from the signing certificate, from the certificate issuer or the date of signing. A verifier of the signature might need some means to verify the correctness of such information by comparing it to the information gained during verifying the signer's identity. In order to do so, the information inside the visible electronic signature needs to be marked up with the semantics of the information by means of some meta-information. This meta-information may be used to link and compare the information from the visible signature to information from a trusted source or to recreate the visible electronic signature with trusted information.

C) Internet X.509 Public Key Infrastructure - Certificate Image: This proposes a means for including images such as a scanned human signature or a company logo into X509-certificates and therefore associated with a certificate. This work is currently underway by the PKIX Working group. (http://www.ietf.org/id/draft-ietf-pkix-certimage-01.txt). This could be a possible trusted source of information for a visible signature.

D) **Positioning of visible signature:** The position of a visible electronic signature inside the electronic document may have a legal bearing, such as indicating the approval of a certain clause of a contract, when it is placed below that clause. This has implications for an automated verification process.

E) **Standard visible signature layout**: Some use cases will require a standardized layout for the information of visible electronic signatures - for example, to make the information contained within easily recognizable by a viewer of the electronic document. This implies means to define templates for visible electronic signatures and to define what information of the electronic signature is displayed where. An example of that use case is done by the Austrian government.

F) **DSS Standard Interfaces for Visible Signatures**: Proposed standards have been produced by the OASIS DSSX Group with the "Visible Signature Profile of the OASIS Digital Signature Services Version 1.0 for networked services supporting the creation of visible signatures. What impact does this have on the requirements for visible signature standards?

G) **Printing visible signatures**: Some use cases may need visible electronic signatures that remain intact even if the electronic document is printed on paper and then scanned again. A printed document displays visible signatures as a part of the part of document which impacts its trustworthiness (see A above).

Responses can be sent by email to: nick.pope@thales-esecurity.com
co-lead STF 364

Response is requested by 12 November 2009